TRANSMITTAL OF APPEAL BRIEF (Large Entity)

Docket No. 67539/00230

In Re Application Of: **VANSTONE, Scott A.**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/360,575	07/26/1999	HOFFMAN, Brandon S.	27871	2136	4374

Invention: **TRANSACTION VERIFICATION PROTOCOL FOR SMART CARDS**

COMMISSIONER FOR PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed on:
April 24, 2006

The fee for filing this Appeal Brief is: **$500.00**

- ☐ A check in the amount of the fee is enclosed.
- ☐ The Director has already been authorized to charge fees in this application to a Deposit Account.
- ☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 02-2553. I have enclosed a duplicate copy of this sheet.
- ☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: **June 26, 2006**

John R.S. Orange (Reg. No. 29,725)
Blake, Cassels & Graydon LLP
Box 25, Commerce Court West
199 Bay Street
Toronto, Ontario M5L 1A9
Canada
Tel: (416) 863-3164
Fax: (416) 863-2653

cc:

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

_____.
(Date)

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

IN THE UNITED STATES PATENT & TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appl. No.: **09/360,575**

Applicant: **Scott Vanstone**

Filed: **July 26, 1999**

Title: **TRANSACTION VERIFICATION PROTOCOL FOR SMART CARDS**

Art Unit: **2136**

Examiner: **HOFFMAN, Brandon S.**

Docket No.: **67539/00230**

Board of Patent Appeals and Interferences
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

I. INTRODUCTION

This is an appeal to the Final Office Action of the Examiner dated January 31, 2006 rejecting claims 9-19. A Notice of Appeal from the Primary Examiner to the Board of Patent Appeals and Interferences was timely filed with the Office on April 24, 2006.

II. REAL PARTY IN INTEREST

The real party in interest in the present application on appeal is Certicom Corp. The present application is a continuation of USSN; 08/790,545; wherein the assignment is recorded in the United States Patent and Trademark Office at Reel 08627, Frame 0863.

III. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences known to the Appellant, Appellant's representative or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

IV. STATUS OF CLAIMS

In this application, claims 1 and 3-8 have been cancelled; in error, claim 2 was never presented; and claims 9-19 are pending. Claims 9-19 are part of the present appeal. Claims 9-19 have been rejected. Please refer to Appendix A for a complete listing of the claims involved in this appeal.

V. STATUS OF AMENDMENTS

An amendment was filed with the Office on November 17, 2005 in response to the non-final rejection mailed May 17, 2005. The claims were amended to clarify the nature of the invention claimed and to include certain limitations recited in the dependent claims. The final rejection which is the subject of this appeal, was then issued on January 31, 2006. No amendments have been filed subsequent to the final rejection.

VI. SUMMARY OF INVENTION

The present invention relates to methods for performing transactions in a communication system. The transactions are performed between a first and second participant (e.g. smart card and card reader respectively – page 4, lines 28-29) whereby the second participant permits a service to be provided to the first participant in exchange for a payment that may be obtained from a third participant (e.g. bank - page 7).

The following example exemplifies the claimed method whilst referring to a card reader (10), smart card (14) and bank, however it will be appreciated that the example is provided for

illustrative purposes only and that the claims shall not be limited by such example.

A transaction is initiated by the smart card (14), e.g., by inserting the smart card into the reader (10). Upon initiation of the transaction, the card reader (10) sends a first message (M1) to the smart card (14). The message (M1) includes information pertaining to the card reader (10). The smart card (14) then verifies the information contained in the first message (M1) to obtain assurance that the service requested by way of the initiated transaction will be provided by the card reader (10) (e.g. cash withdrawal, receipt of merchandise etc.) upon the smart card (14) assuring that the card reader (10) may obtain payment for the service.

The smart card (14) prepares a second message (M2) and sends the second message (M2) to the card reader (10). The second message (M2) includes information pertaining to the smart card (14) including a digital signature (having components r1, s1) that is later used by the card reader (10) to obtain payment. The card reader (10) verifies the second message (M2) to obtain assurance that the payment will be secured upon provision of the service. Therefore, the smart card (14) and the reader (10) first verify each other's identity using the passage of a message in each direction (M1, M2). Once the information pertaining to the smart card (14) is verified by the card reader (10), the card reader (10) obtains the digital signature from the second message (M1) and uses the digital signature (having components r1, s1) to obtain payment from the bank for providing the service.

Accordingly, the computation required by the smart card (14) is minimal, being restricted to one verification and the preparation of one signature (included in the second message), with the balance avoiding computationally intense operations (e.g. see page 6, lines 22-25). Therefore, it has been recognized by the inventors that the steps recited in the claims provide security for the transaction whilst minimizing the computational burden on the smart card (14), which is of paramount importance. It is the sequence of passes of messages (M1, M2) and the use of a digital signature (having components r1, s1) of the smart card (14) that enables such a balance to be achieved.

VII. THE FINAL REJECTION

Claims 9-19 are currently pending in this application and stand rejected. The following discusses each rejection in the order addressed in the Final Office Action.

In the Final Action mailed January 31, 2006, the Examiner rejected claims 9-14, 18 and 19 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,396,558 to Ishiguro et al. (hereinafter "Ishiguro") in view of U.S. Patent No. 6,069,952 to Saito et al. (hereinafter "Saito").

The Examiner has stated that the Appellant's arguments with respect to claims 9-19 filed November 17, 2005 have been fully considered but were found to not be persuasive. The Examiner maintains that Ishiguro teaches the subject matter of claim 9 minus the provision that "...upon verification of said information pertaining to said first participant, said second participant obtaining a digital signature for said first participant on said transaction using said second message...". The Examiner believes that Saito teaches what is missing from Ishiguro and that as such, it would have been obvious to combine the teachings of Saito with the system of Ishiguro "...because the digital signature protects the communication between the IC card and terminal from a replay attack, which is a common attack to defraud unprotected businesses and customers." The Appellant respectfully traverses the Examiner's rejections.

The Examiner has rejected claims 15-17 under 35 U.S.C. 103(a) as being unpatentable over Ishiguro in view of Saito, in further view of U.S. Patent No. 5,276,736 to Chaum. (hereinafter "Chaum").

The Examiner believes that Ishiguro and Saito, in combination, fails to teach the limitation pertaining to third and fourth message as recited in claims 15-17 but that Chaum meets such limitations and, as such claims 15-17 would thereby be rendered obvious in further view of Chaum. The Appellant respectfully traverses the Examiner's rejections.

VIII. ISSUES

The issues on appeal in this matter are:

1. whether claims 9-14, 18 and 19 are unpatentable under 35 U.S.C. 103(a) over Ishiguro in view of Saito; and
2. whether claims 15-17 are unpatentable under 35 U.S.C. 103(a) over Ishiguro in view of Saito, in further view of Chaum.

IX. GROUPING OF CLAIMS

The Appellant considers the claims to be separately patentable and, as such, respectfully submits that the claims do not stand or fall together.

X. APPELLANT'S ARGUMENTS

As discussed above in section VI, the second correspondent (e.g. card reader) obtains a digital signature from the second message and uses the digital signature to obtain payment from a third party (e.g. bank) for providing a service. Such limitations are clearly recited in claim 9.

In the method recited in claim 9, the computation required by the first participant (e.g. smart card) is minimal, being restricted to one verification and the preparation of one signature (included in the second message), with the balance avoiding computationally intense operations (e.g. see page 6, lines 22-25).

It has been recognized by the inventors that the sequence of steps recited in the claims are capable of securing the transaction whilst minimizing the computational burden on the first participant (e.g. smart card), which is of paramount importance, especially where computational power is at a minimum. It is the sequence of passes of messages and the use of the digital signature in the second message that enables such a balance to be achieved.

Claims 9-14, 18 and 19 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro in view of Saito. The Appellant respectfully traverses the rejections as follows.

The Appellant will show, as follows, that neither Ishiguro nor Saito, alone or in combination teach a step of using a digital signature from a second message to obtain payment from a third participant, let alone the sequence of steps that results in the secure transaction provided by the method claimed. Further, the Appellant will show that, if one were to incorporate the teachings of Saito in the system taught by Ishiguro, at best, a digital signature would be included in each pass, i.e. a computational burden, which is what the present invention intends to avoid. Further still, Ishiguro teaches how to avoid using a third party and thus teaches away from what the Examiner believes would be obvious to include.

Ishiguro teaches a method for performing a transaction with an IC card and a terminal.

The method involves successive passes of information between the card and the terminal, wherein a digital signature is verified on each pass. The Examiner relies on column 2, lines 42 to 56. In this passage, Ishiguro teaches the IC card sending a card ID number and a first master signature to the terminal, the terminal verifies the first master signature, if valid the terminal transmits a terminal ID number and a second master signature to the IC card, the IC card verifies the second master signature and, if valid, the IC card generates a value V corresponding to the charge for a service after the service is provided. Ishiguro does not teach of the terminal using a digital signature to obtain payment from a third party, but in fact teaches away from using a third party. The Appellant acknowledges that Ishiguro mentions a third party but submits that Ishiguro intends to avoid interacting with such third party. As clearly stated in column 2, lines 20-25, "...which eliminate the need for communication between the management center and the IC card terminal each time the card user inserts his IC card into the latter to get his desired service...". Based on this motivation, Ishiguro teaches sending and verifying a digital signature at each pass to avoid the use of a third party.

Clearly, Ishiguro teaches away from incorporating what is missing from the steps recited in claim 9. In fact, Ishiguro is not concerned with minimizing a computational burden on the IC card but rather is concerned with avoiding the need to obtain payment from a third party. There is simply no motivation to modify Ishiguro when it is clear from the teachings that Ishiguro intends to not include a third party. Moreover, since Ishiguro teaches away from incorporating a third party, there is nothing in the teachings that provides direction as to how to incorporate the third party, let alone as recited in claim 9.

The Examiner admits that Ishiguro "...does not teach upon verification of said information pertaining to said first participant, said second participant obtaining a digital signature...may obtain payment from a third participant using said digital signature.". The Examiner believes that Saito teaches such a limitation and, as such, it would be obvious to combine the teachings of Saito within the system of Ishiguro as discussed above in section VII.

Saito teaches, in part, a transaction system and method, involving a bank, customer, and retail shop as shown in Figure 8 and described in columns 39-42 (relied upon by the Examiner). Essentially, the customer uses a terminal to request an amount of digital cash from the bank and sends a customer ID number. The bank receives the request and encrypts the cash with a first key. The customer receives the encrypted amount and confirms the content using the first key.

The customer generates a second key and encrypts the cash with the same. The customer may then decrypt the cash using the second key when a purchase is conducted. The retail shop receives the encrypted cash from the customer and obtains the second key through its bank and the customer's bank. The retail shop obtains the second key and decrypts the cash to confirm the amount. Once confirmed, an article of desire is transferred to the customer.

The Examiner relies, in particular on column 42, lines 55-58 wherein Saito states that digital signatures are beneficial during any of the above communications. The Examiner equates the bank taught by Saito to the third participant recited in claim 9. If one were to follow this logic then Saito teaches a step of the customer requesting digital cash from the bank and then the customer effects payment to the retail shop. A careful review of claim 9 would indicate that what is recited therein is in fact opposite to what is taught by Saito. In the example provided above pertaining to claim 9, the card reader obtains payment from a third party using a digital signature whereas in Saito, the customer (e.g. card) obtains the electronic cash and then the retail shop decrypts the cash and completes the transaction.

Therefore, even though Saito teaches a third participant, the third participant is not involved in the same way as recited in claim 1. Moreover, Saito only states that digital signatures would be beneficial at each pass, however, this would only reasonably be interpreted as suggesting that for maximum security, digital signatures should be included in each pass. Saito simply does not teach the sequence of steps that limits the computational burden on the first participant to a verification and a signature as claimed in the present application.

The Appellant respectfully submits that it is improper to rely on hindsight to make a reference say something more than it actually says. The Appellant believes that, with the benefit of the present application, the Examiner has made a leap of logic in reading too much into the teachings of Saito. Saito does not provide direction as to how the second participant (e.g. retailer, card reader) can use a digital signature to effect payment from a third participant. There is no direction and thus no motivation to incorporate such an undisclosed sequence of steps. Further, as the Appellant is believed to have shown, Ishiguro actually teaches away from incorporating a third participant and thus there is no link between the two references that would lead a person skilled in the art towards such a combination.

The Appellant believes that neither Ishiguro, nor Saito, alone or in combination, teaches the sequence of passes recited in claim 9 that achieve the above-noted balance between

computational burden and security in the transaction. The Appellant also believes that there is no direction in either reference to modify Ishiguro to incorporate a third participant. In fact, Ishiguro teaches away from utilizing a third participant and neither reference teaches how such a transaction could be implemented.

As noted above, Ishiguro uses a digital signature verification at each step to increase security. It would be contrary to those teaches to use a digital signature only in a second message for obtaining payment. Similarly, Saito is silent as to how to reduce computational burden and intends to provide a cryptographic function in each pass.

Accordingly, the Appellant believes that the combination of Ishiguro and Saito is an unlikely one, which even if combined would not render claim 9 obvious. As such, the Appellant believes that claim 9 is patentable for at least that reason.

Claims 10-19 being ultimately dependent on claim 9 are also believed to be patentable.

Claims 15-17 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro in view of Saito, in further view of Chaum. The Appellant respectfully traverses the rejections as follows.

Chaum teaches the provision of a "challenge" wherein a digital signature is obtained based on the messages exchanged during the challenge. However, Chaum does not teach a step of obtaining a digital signature on a message sent from the first participant to the second participant, wherein the digital signature is used to obtain payment from a third participant, i.e., what the Appellant is believed to have shown is missing from both Ishiguro and Saito. Therefore, Chaum does not teach what is missing from Ishiguro and Saito and, for at least that reason, claims 15-17 are believed to be patentable over the references cited by the Examiner.

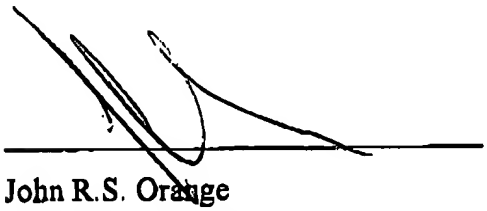
XI. CONCLUSION

In view of the foregoing, the Appellant is believed to have shown that the Examiner has erred in finding claims 9-14, 18 and 19 as being unpatentable over Ishiguro in view of Saito. The Appellant is also believed to have shown that the Examiner has erred in finding that claims 15-17 are unpatentable over Ishiguro in view of Saito, in further view of Chaum.

Accordingly, the Appellant respectfully submits that claims 9-19 clearly and patentable distinguish over the references cited by the Examiner and are in condition for allowance.

Therefore, the Appellant respectfully requests that this honorable Board of Patent Appeals and Interferences reverse the Examiner's decision in this case and indicate the patentability of claims 9-19 in this application.

Respectfully submitted,



John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: 26 June 2006

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164
JRO/BSL

APPENDIX A – Claims on Appeal

Listing of claims under appeal:

1. (cancelled)

2. (not presented)

3. - 8. (cancelled)

9. (previously presented) A method of performing a transaction in a communication system between a first and a second participant wherein said second participant permits a service to be provided to said first participant in exchange for a payment, said method comprising the steps of:

a) upon initiation of said transaction by said first participant, said second participant sending a first message to said first participant, said first message including information pertaining to said second participant;

b) said first participant verifying said information pertaining to said second participant to obtain assurance that said service will be provided upon assuring said payment;

c) said first participant sending a second message to said second participant, said second message including information pertaining to said first participant;

d) said second participant verifying said information pertaining to said first participant to obtain assurance that payment will be secured upon provision of said service; and

e) upon verification of said information pertaining to said first participant, said second participant obtaining a digital signature for said first participant on said transaction using said second message, whereby said second participant may obtain said payment from a third participant using said digital signature.

10. (previously presented) A method according to claim 9 wherein said first participant is a holder of a card which performs cryptographic operations.

11. (previously presented) A method according to claim 10 wherein said second participant is a terminal.

12. (previously presented) A method according to claim 11 wherein said third participant is a financial institution.

13. (previously presented) A method according to claim 9 wherein said information pertaining to said second participant included in said first message includes details and credentials of said second participant; and said first participant verifies said details and said credentials in step b).

14. (previously presented) A method according to claim 9 wherein said information pertaining to said first participant included in said second message includes details and credentials of said first participant; and said second participant verifies said details and credentials in step d).

15. (previously presented) A method according to claim 9 wherein said second message includes a challenge and step e) further comprises:

i) said second participant generating a response to said challenge;

ii) said second participant sending a third message including said response to said first participant;

iii) said first participant verifying said response; and

iv) said first participant sending a fourth message to said second participant such that said digital signature is provided by said second message and said fourth message.

16. (previously presented) A method according to claim 15 further comprising:

i) said second participant verifying information in said fourth message;

ii) said second participant completing said transaction by providing said service; and

iii) said second participant sending said third participant a subset of said first, second, third and fourth messages to obtain said payment.

17. (previously presented) A method according to claim 16 further comprising:

i) said third participant verifying said subset;

ii) said third participant providing said payment to said second participant.

18. (previously presented) A method according to claim 13 wherein said credentials include a public key certificate.

19. (previously presented) A method according to claim 15 wherein said challenge is a nonce.

APPENDIX B – Evidence

[None]

APPENDIX C – Evidence

[None]